Indian Journal of Science and Technology, Vol 9(38), DOI: 10.17485/ijst/2016/v9i38/101283, October 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Recent Approaches for VoIP Steganography

Ahmed Hussain Ali[1*], Mohd Rosmadi Mokhtar[1] and Loay Edwar George[2]

[1]Faculty of Information Science and Technology, University Kebangsaan Malaysia, 43600 Bandar Baru Bangi, Malaysia; ahmedhussainali78@gmail.com
[2]Department of Computer Science, College of Science, University of Baghdad, Baghdad, Iraq

Abstract

Background/Objectives: With the development of data communication, it is essential to find a way to keep the important and secret data during transmission through the internet or mobile communications. Steganography is the most popular technique that is used in information hiding. In steganography, the secret information is embedded inside a cover file or carrier without effect on the quality of that cover file. The carriers used in steganography can be classified into two types: A static digital carrier such as text, image, audio and video files that are applied in digital steganography, and instant or dynamic carrier like an audio stream or network protocol called network steganography. Network steganography is a relatively modern trend in information hiding. It utilizes the development in network functionality and services to convey the secret data. Voice over Internet Protocol (VoIP) is the most common service that is adoptedby researchers in respect to information hiding. **Methods/Statistical Analysis:** This paper presents a brief review of features, classification and recently proposed network steganography technique. **Findings:** Many efforts nowadays are exerted to develop the LSB-VoIP techniques and adopting other techniques along with LSB to improve the steganography efficiency regarding hiding capacity and imperceptibly.

Keywords: Audio Codec, G.711, LSB, Steganography, VoIP

1. Introduction

For many decades, security and authentication have been critical challenges due to the nature of digital communication. Cryptography was an ancient technique that can protect the secret data by encrypted the secret file. Steganography was another concept that has the advantage of hiding the presence of the message in such a way that no one other than the sender and intended receiver sense its existence. It can be considered as information smuggling[1]. Many steganography researches focus on hiding information in text[2,3], image [4,5], audio[6,7] and video[8] files. Techniques using those files as a cover file called digital steganography. With the growing of network protocol and services, the researchers direct their interest toward adopting techniques for the real-time carrier to increase the security and put difficulties against data eavesdropping, which is called Network Steganography. VoIP service took up most of the attention because the additional security that is provided because these techniques are real time and do not give the warden adequate time to discover the secret data. Moreover, stream data are a suitable carrier because of the dynamic and variable length for hiding the data which is relatively larger than traditional files[9].

2. Features

Network steganography required to make a trade-off between three key features: Bandwidth, security, and robustness. Bandwidth points to the size of data that can be sent per time unit, which is equivalent to capacity in digital steganography and many researchers try to achieve as high bandwidth as possible. Security can be defined as a measure for detecting secret data in a particular carrier. The orientation toward network steganography is

*Author for correspondence

to enhance this feature. Robustness means the ability to resist modification or alteration on the carrier[9]. As for network steganography,[10] spotlighted the feature that can measure degradation in network functionality which is called cost. It is a criterion for the degradation in VoIP conversation or the protocol's facility when using network protocols. Steganography technique can be considered ideal if it fulfills the balance between these requirements of being robust, uneasy to detect and having high hiding capacity.

3. VoIP Steganography

Hiding information in VoIP streaming is highlighted in the research community with the spreading and increasing of using VoIP applications. Several embedding techniques were employed in the literature; however, LSB the most common technique was used due to being low complexity, high capacity and simple to implement. It adopted LSB's of the speech stream samples in incorporating the secret message into VoIP speech. All the efforts focus on improving the steganography transparency, capacity and security.

Author in[11] proved that embedding transparency can be enhanced when they use voiced packets (not silent) in embedding using silence detection. They used key between sender and receiver to generate a random number which is used in selection LSB bits. The capacity of this study depends mainly on the sample rate.

Author in [12] proposed a scheme for hiding speech in a real-time communication system using the G.711 codec which is widely supported by VoIP. The scheme adopts Speex to compress the secret speech to 8 kHz and reduce the time before embedding into the packet. Despite this schema compress the secret speech, the hiding capacity is relatively moderate. It chooses half of 8 bits cover speech sample to reduce the dramatic modification during hiding.

Steganography algorithm based on LSB matching that hides secret data over VoIP was adopted by[13]. It used a pseudo-random number of select cover samples and guided for embedding. They suggested a mechanism for packet loss problem using secret message retransmission. They evaluate the algorithm using speech codec G7.11 and Stega-Talk software [13].

presented a secure and real-time model for covert communication for VoIP using LSB technique and encryption. They used G.729a as a coder of covered speech in StegTalk to evaluate the performance of the model. The model hides only 0.8 kb/s and 2.6 kb/s of secret message. This model needs for further improvement to increase the capacity [14].

Enhanced algorithm for embedding transparency was proposed by[15]. It depends on the Partial Similarity Value (PSV) between the LSB of G.729a codec and a secret message. It makes a balance between transparency and capacity. The capacity depends on the number of comparable bits and threshold; the result shows the best embedding efficiency when using 4 bits and similarity threshold is 3 with 1444 bits in 126 frames. The similarity parameters and the time required for the proposed algorithm require further enhancements.

A model for real-time VoIP steganography with ITU-T G.729a cover speech codec was proposed by [16]. This method was used to make a balance between good security and real-time performance. It adopts LSB substitution approach with M-sequence to reduce the correlation between secret message and RSA key synchronization for accurate secret message recovery. The result showed good performance and the adequate real-time requirement for VoIP.

Author in[17] presented a steganography approach that is applied to a coded parameter of G.723.1 low bit rate coded speech. It adopts 5-LSB's of each coded speech frame for embedding secret information, augmented identity matrix to minimize the modification of cover speech and encryption. It is simple, effective, and has low computational complexity. The frame length of G.723.1 is 240 samples (30 seconds with 8 kHz sample rate) 5.3Kbps. Further work is to enhance capacity and robustness[17].

Author in[18] proposed data hiding technique that adopts the LSB substitution method and estimation tolerable distortion in G.711 codec speech. The result shows the technique outperforms LSB and selective embedding proposed[19] with 4kbps with no distortion and 10 kbps with high quality. The embedding rate is 5585 bps using 32 Kbits/s.

A covert communication system in G.711 stream in VoIP was proposed by[20]. It uses LSB method and VoIP stream for embedding and adopts a strategy to hide higher embedding rate in the sharp blocks in comparison with the flat blocks to avoid detection. The result shows that the proposed system can avoid RS detection and the degradation MOS -LQO value is 4.07 and high hiding capacity around 7.43kbps.

Steganography schema in VoIP was presented in[21] that adopted an adaptive Partial Matching Steganography (PMS) for matching the similarity between secret message and cover. The encryption is integrated with the embedding process to reduce delay. The triple M-sequence is used in this schema. They evaluated the proposed approach with ITU-T G.729a as the codec for cover speech in StegVoIP. The tradeoff between the transparency and the capacity depend on the M sequence and the bandwidth between 1.05 and 5.97 bit per frame.

Table 1. Summary of the selected studies

Reference	Methodology	Contribution
2006[11]	Distributed LSB, Silent detection, encryption, PCM	Improve the transparency and security
2007[12]	LSB, Speex compression, G.711	Enhance capacity and process time
2008[13]	LSB matching, packet loss mechanism, G7.11	Increase security and stego quality, proposed solution for packet loss problem
2008[14]	LSB, encryption, G.729a	Increase transparency and security
2009[15]	LSB, partial similarity value (PSV), G.729a	Balance between transparency and hiding capacity
2009[16]	LSB, M-sequence encryption, synchronization mechanism RSA, G.729a	Balance between transparency, security and latency
2009[17]	LSB, augmented identity matrix, encryption, G.723.1	Balance between transparency and complexity
2010[18]	LSB, estimate of tolerable distortion, G.711	Enhance transparency and hiding capacity
2011[20]	LSB, checking smoothness blocks, G.711	Increase security, speech quality and hiding capacity
2011[21]	LSB, Partial Similarity Value (PSV), M-sequence, G.729a	Balance between transparency and hiding capacity
2014[22]	LSB, variable capacity, AES-128 encryption, PCM	Increase security and transparency
2014[1]	LSB, three approaches VAMI, VODO and (VADDI), G.711	Enhance security and transparency
2015 [23]	LSB, Adaptive Partial Matching Steganography (APMS), G.711	Balance between transparency and hiding capacity

Author in[22] proposed a real-time covert communication system that embeds the secret message into VoIP audio packets. The secret message is first encrypted using symmetric cryptography AES-128 and symmetric key that is shared with the receiver in SIP protocol before the embedding process. Then the encrypted secret message is embedded into audio packets encoded by PCM codec using distributes LSB before sending it to the dedicated receiver. It used variable embedding capacity depending on the embedding algorithm that is used.

An adaptive approach for embedding secret data into VoIP audio stream was proposed. It adopts G.711 audio codec to evaluate the efficiency. It is used to enhance the security of the direct LSB embedding bits that exists in the systems by adopting three techniques: Value-based Multiple Insertion (VAMI) and Voice Damage Offset (VODO) and Voice Activity Detection Dynamic Insertion (VADDI). It showed better transparency, however, its bandwidth average is low around 102.28 bps.

Author in[23] proposed an improved Adaptive Partial Matching Steganography (APMS) to make a balance between transparency and bandwidth for steganography in VoIP by matching the similarity between the cover and secret files. They adopted three aspects to make the enhancement: first adopting unequal probability to enhance the transparency, second using matrix embedding for unused cover parts to increase the capacity and third more encryption for the secret messages to increase the embedding efficiency. They used ITU-TG 711 (a-low) as a cover speech to evaluate the proposed strategy. The

result showed that the capacity is between 1 to 6 kbps. Table 1 presents a summary of the above-selected studies.

4. Conclusion

Network steganography is a modern technique that exploits the network headers, protocols and services for creating covert channels to transmit secret information over a network. VoIP streaming plays a major role in information hiding with the increasing use of VoIP applications. This study turns the way towards the techniques that utilize LSB in VoIP streaming especially with the G.711 audio codec. The interesting in using G.711 is the consequence of the popularity of using IP telephony in addition to the simplicity, high capacity and low complexity of the LSB. Many efforts are still dedicated to improving LSB-VoIP techniques in terms of hiding capacity and imperceptibly. Further work is required to cover the latest techniques that are adopted in VoIP steganography beside the LSB techniques that are discussed in this study. This will give a clear idea about the limitation in network steganography approaches.

5. References

1. Wei Z, Zhao B, Liu B, Su J, Xu L, Xu E. A novel steganography approach for voice over IP. Journal of Ambient Intelligence and Humanized Computing. 2014 Aug; 5(4):601–10.
2. Roy S, Venkateswaran P. A text based steganography technique with indian root. Procedia Technology. 2013 Dec; 10:167–71.
3. Kingslin S, Kavitha N. Evaluative approach towards text steganographic techniques. Indian Journal of Science and Technology. 2015 Nov; 8(29):1–8.
4. Hemalatha S, Acharya UD, Renuka A, Kamath PR. A secure and high capacity image steganography technique. Signal and Image Processing: An International Journal (SIPIJ). 2013 Feb; 4(1):83–9.
5. Somassoundaram T, Subramaniam N. High capacity image steganography using secret key for medical information. Indian Journal of Science and Technology. 2016 Jan; 9(3):1–5.
6. Kar DC, Mulkey CJ. A multi-threshold based audio steganography scheme. Journal of Information Security and Applications. 2015 Aug; 23:54–67.
7. Shahadi HI, Jidin R, Way WH. Lossless audio steganography based on lifting wavelet transform and dynamic stego key. Indian Journal of Science and Technology. 2014 Mar; 7(3):323–34.
8. Ramalingam M, Isa NAM. Video steganography based on integer haar wavelet transforms for secured data transfer. Indian Journal of Science and Technology. 2014 Jul; 7(7):897–904.
9. Mazurczyk W. VoIP steganography and its detection- A survey. ACM Computing Surveys (CSUR). 2013 Nov; 46(2):1–21.
10. Mazurczyk W, Wendzel S, Villares IA, Szczypiorski K. On importance of steganographic cost for network steganography. Security and Communication Networks. 2016 May; 9(8):781–90.
11. Kraetzer C, Dittmann J, Vogel T, Hillert R. Design and evaluation of steganography for voice-over-IP. Proceedings 2006 IEEE International Symposium on Circuits and Systems; 2006 May.
12. Wang C, Wu Q. Information hiding in real-time VoIP streams. 2007 9th IEEE International Symposium on Multimedia, 2007 ISM; 2007 Dec. p. 255–62.
13. Huang Y, Xiao B, Xiao H . Implementation of covert communication based on steganography. 2008 IIHMSP'08 International Conference on Intelligent Information Hiding and Multimedia Signal Processing; 2008 Aug. p. 1512–5.
14. Tian H, Zhou K, Huang Y, Feng D, Liu J. A covert communication model based on least significant bits steganography in voice over IP. The 9th International Conference for Young Computer Scientists; 2008 Nov. p. 647–52.
15. Tian H, Zhou K, Jiang H, Huang Y, Liu J, Feng D. An adaptive steganography scheme for voice over IP. 2009 IEEE International Symposium on Circuits and Systems, 2009 ISCAS; 2009 May. p. 2922–5.
16. Tian H, Zhou K, Jiang H, Liu J, Huang Y, Feng D. An m-sequence based steganography model for voice over IP. IEEE International Conference on Communications, 2009 ICC'09; 2009 Jun. p. 1–5.
17. Xu T, Yang Z. Simple and effective speech steganography in G. 723.1 low-rate codes. 2009 International Conference on Wireless Communications and Signal Processing; 2009 Nov. p. 1–4.
18. Ito A, Abe S, Suzuki Y. Information hiding for G.711 speech based on substitution of least significant bits and estimation of tolerable distortion. *2009 IEEE International Conference on Acoustics, Speech and Signal Processing;* 2009 Apr. p. 1409–12.
19. Aoki N. A band extension technique for G.711 speech using steganography. IEICE transactions on communications. 2006 Jun; 89(6):1896–8.
20. Miao R, Huang Y. An approach of covert communication based on the adaptive steganography scheme on voice over IP. 2011 IEEE International Conference on Communications (ICC); 2011 Jun. p. 1–5.

21. Tian H, Jiang H, Zhou K, Feng D. Adaptive partial-matching steganography for voice over IP using triple M sequences. Computer Communications. 2011 Dec; 34(18):2236–47.
22. Tang S, Jiang Y, Zhang L, Zhou Z. Audio steganography with AES for real-time covert voice over internet protocol communications. Science China Information Sciences. 2014 Feb; 57(3):1–14.
23. Hui T, Jie Q, Shuting G, Yongfeng H, Jin L, Tian W. Improved adaptive partial-matching steganography for voice over IP. Computer Communications. 2015 Oct; 70(C):95–108.